UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/815,518	04/01/2004	David Fultz	IDF 2564 (4000-15700)	8230

28003 7590 04/07/2008
SPRINT
6391 SPRINT PARKWAY
KSOPHT0101-Z2100
OVERLAND PARK, KS 66251-2100

EXAMINER
ABEDIN, SHANTO

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
04/07/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/815,518	**Applicant(s)** FULTZ ET AL.	
	Examiner SHANTO M Z ABEDIN	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *03* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 January 1933*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-33* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This office action is in response to the communication filed on 12/27/2007.

2. Claims 1-33 are currently presented for the examination.

3. Claims 1-33 have been rejected.

Response to Arguments

4. The applicant's arguments regarding 35 USC 103 (a) type rejections are fully considered, however, found not persuasive since combination of references Upton and Beck et al does teach the limitations set forth by the arguments.

In particular, firstly, reference Upton teaches wherein the token contains user credentials encoded as a platform and application independent primitive data type (Fig 4; Par [0104], [0114], [0130], [0150]; Claims 1,12; generic/ token type credentials), and reference Beck et al teaches the authentication authority further operable to generate a token, and wherein the token contains user credentials encoded as a platform and application independent primitive data type (Par [0019]-[0024]; generating the user id token that would be used for authentication).

Secondly, the examiner respectfully disagrees with the applicant's arguments regarding the properness of combining references Upton and Beck. In response to the applicant's arguments that combination of Upton and Beck would result in an insecure environment, the examiner notes, references do not suggest teaching away from each others or such deficiencies, and the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981).

5. However, upon further search and examination, new grounds of rejection are found, and the applicant's arguments are moot in view of new grounds of rejection presented in this office action.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-3, 9-12, 24, 28 and 29 are rejected under 35 USC 103 (a) as being unpatentable over Upton (US 20030097574 A1) in view of Beck et al (2004/0088349 A1) further in view of O'Donnell et al (US 2004/0117615 A1)

Regarding claim 1, Upton discloses a system to provide application-to-application enterprise security, the system comprising:

a security application program interface coupled to a client application operable on a first operating system to provide a security credential (Par [0061]-[0074], [0127]-[0130]; Claims 1 and 12; client application/ interface);

an authentication authority (Par [0115],[0128]-[0130], [0145]-[0147]; security services; authentication/ authorization SPI) receiving the security credential from the security application program interface, the authentication authority further operable to communicate the token to the security application program interface where the security credential is valid, wherein the token contains user credentials encoded as a platform and application independent primitive data type (Fig 4; Par [0104], [0114], [0130], [0150]; Claims 1,12; service provider interface/ SPI; checking public/ password type, or generic/ token type credentials).

a store maintaining data validating the security credential, the store in communication with the authentication authority to validate the security credential (Par [0065]-[0066]; storing credential/ passwords);

an application program interface coupled to the client application, the application program interface operable to communicating regarding the validating of the token (Par [0061]-[0074], [0104], [0114], [0130], [0150]; claims 1,12; client application/ interface using credentials/ token for mapping/ authentication) and

a server application operable on a second operating system to receive the token from the application program interface, the server application communicating with
the authentication authority to validate the token to enable the client application to
use services of the server application (Par [0104], [0114]-[0116], [0130]; Claims 1,12; 3rd party validating/ authenticating credentials).

Although Upton discloses use of a token as credentials (Par [0150]), and it would be further logically obvious to an ordinary skill in art to generate the token , Upton fails to disclose expressly the authentication authority further operable to generate a token.

However, Beck et al discloses the authentication authority further operable to generate a token (Par [0019]-[0024]; generating the user id token that would be used for authentication).

In the case position for inherency is not found supportable, the examiner notes that the reference O'Donnell et al discloses the authentication authority further operable to generate a token (Par [0061]-[0070]; Claims 1-40; access/ application server generating, and sending authentication token to user upon validation of the credential). O'Donnell et al further discloses an authentication authority receiving the security credential from the security application program interface, the authentication authority further operable to communicate the token to the security application program interface where the security credential is valid, wherein the token contains user credentials encoded as a platform and application independent primitive data type (Par [0061]-[0070]; Claims 1-40).

O'Donnell et al , Beck et al and Upton are analogous art because they are from the same field of authentication for network/ enterprise services. At the time of invention, it will be obvious to a person with ordinary skill in the art to combine the teaching of O'Donnell et al and/ or Beck et al with Upton to design the system wherein the authentication authority further operable to generate a token in order to facilitate an anonymous token based authentication.

Regarding claim 9, it is rejected applying as same motivation and rationale as applied above rejecting claim 1, furthermore, Upton discloses A method for providing application-to-application enterprise security, the method comprising:

communicating a security credential from a client application operable on a first operating system to an authentication authority (Par [0061]-[0074], [0127]-[0130], [0130], [0150]; Claims 1,12; client application/ interface providing credentials; service provider interface/ SPI authenticating public/ password type, or generic/ token type credentials);

communicating information related to the security credential between the authentication authority and a data store to determine whether the security credential is valid; wherein the token contains user credentials encoded as a platform and application independent primitive data type (Par [0104], [0114], [0130], [0150]; Claims 1,12; service provider interface/ SPI; validating/ authenticating credentials);

communicating the token to the client application; providing, by the client application, the token to a server application, the server application operable on a second operating system (Par [0061]-[0074], [0127]-[0130], [0130], [0150]; Claims 1,12; client application/ interface providing credentials; service provider interface/ SPI authenticating public/ password type, or generic/ token type credentials) ; and

validating, by the server application, the token before providing access to services of the server application by the client application (Par [0104], [0114]-[0116], [0130]; Claims 1,12; 3rd party validating/ authenticating credentials).

Upton fails to disclose expressly generating a token by the authentication authority when the security credential is valid.

However, Beck et al discloses generating a token by the authentication authority when the security credential is valid (Par [0024]; generating the token that would be used for authentication).

In the case position for inherency is not found supportable, the examiner notes that the reference O'Donnell et al discloses the authentication authority further operable to generate a token, wherein the token contains user credentials encoded as a platform and application independent primitive data type (Par [0061]-[0070]; Claims 1-40; access/ application server generating, and sending authentication token to user upon validation of the credential). O'Donnell et al further discloses communicating the token to the client application; and validating by the server application, the token before providing access to server application by the client application (Par [0061]-[0070]; Claims 1-40).

Regarding claim 28, it recites the limitations of claims 1 and 9, therefore, it is rejected applying as above rejecting claim 1 and 9.

Regarding claim 2, Upton discloses the system of Claim 1, wherein the server application further comprises: an application program interface to communicate with the application program interface of the client application (Par [0061]-[0074], [0127]-[0130]; Claims 1 and 12; client application/ interface); and a security application program interface to communicate with the authentication authority (Par [0115],[0128]-[0130], [0145]-[0147]; security services; authentication/ authorization SPI).

Regarding claim 3, Beck et al discloses wherein the server application is operable to cache the token after validating the token with the authentication authority such that when the client application requests service of the server application, via the application program interfaces of the client application, the server application uses the cached token to validate the client application (Par [0018]-[0120]; using generated/ stored token for authentication).

Regarding claims 10-12 and 29, they recite the limitations of claims 1-3, 9 and 28, therefore, they are rejected applying as above rejecting claims 1-3, 9 and 28.

Regarding claim 24, Upton discloses wherein the security credential is further defined as including a password and user identification (Par [0061]-[0074], [0150]).

7. Claims 8 and 15 are rejected under 35 USC 103 (a) as being unpatentable over Upton (US 20030097574 A1) in view of Beck et al (2004/0088349 A1) further in view of O'Donnell et al (US 2004/0117615 A1) further in view of Laferriere et al (US 2005/0188212 A1).

Regarding claim 8, modified Beck et al -Upton system fails to disclose wherein validating the token by the authentication authority includes determining whether the authentication authority created the token.

However, Laferriere et al discloses wherein validating the token by the authentication authority includes determining whether the authentication authority created the token (Par [0012]-[0023]; claims1,14).

Laferriere et al and Upton are analogous art because they are from the same field of authentication for network/ enterprise services. At the time of invention, it will be obvious to a person with ordinary skill in the art to combine the teaching of Laferriere et al with modified O'Donnell et al -Beck et al -Upton to design the system wherein validating the token by the authentication authority includes determining whether the authentication authority created the token in order to provide credential security through authenticating the credential provider.

Regarding claim 15, it recites the limitations of claim 8 and 9, therefore, it is rejected applying as above rejecting claims 8 and 9.

8. Claims 26-27 are rejected under 35 USC 103 (a) as being unpatentable over Upton (US 20030097574 A1) in view of Beck et al (2004/0088349 A1) further in view of O'Donnell et al (US 2004/0117615 A1) further in view of Favazza et al (US 20040139319 A1).

Regarding claim 26, Upton discloses data store is a certificate authority (Par [0076]-[0077]), however, modified O'Donnell et al -Beck et al -Upton system fails to disclose wherein the security credential is an X.509 certificate.

However, Favazza et al discloses w wherein the security credential is an X.509 certificate (Par [0039], [0050]).

Favazza et al and Upton are analogous art because they are from the same field of authentication for network/ enterprise services. At the time of invention, it will be obvious to a person with ordinary skill in the art to combine the teaching of Favazza et al with modified O'Donnell et al -Beck et al -Upton to design the system wherein the security credential is an X.509 certificate to provide alternative secure credentials.

Regarding claim 27, it is rejected applying as above rejecting claim 26, furthermore, Upton discloses communicating the X.509 certificate from the authentication authority to the certificate authority (Par [0073], [0076]-[0077]); validating the certificate by the certificate authority; and communicating validation information to the authentication authority (Par [0073], [0076]-[0077]).

however, modified Beck et al -Upton system fails to disclose wherein the security credential is an X.509 certificate.

However, Favazza et al discloses wherein the security credential is an X.509 certificate (Par [0039], [0050]).

9. Claims 1-7, 9-14, 16-25 and 28-33 are rejected under 35 USC 103 (a) as being unpatentable over Upton (US 20030097574 A1) in view of Beck et al (2004/0088349 A1) further in view of Bhat et al (US 2003/0200465 A1)

Regarding claim 1, Upton discloses a system to provide application-to-application enterprise security, the system comprising:

a security application program interface coupled to a client application operable on a first operating system to provide a security credential (Par [0061]-[0074], [0127]-[0130]; Claims 1 and 12; client application/ interface);

an authentication authority (Par [0115],[0128]-[0130], [0145]-[0147]; security services; authentication/ authorization SPI) receiving the security credential from the security application program interface, the authentication authority further operable to communicate the token to the security application program interface where the security credential is valid, wherein the token contains user credentials encoded as a platform and application independent primitive data type (Fig 4; Par [0104], [0114], [0130], [0150]; Claims 1,12; service provider interface/ SPI; checking public/ password type, or generic/ token type credentials).

a store maintaining data validating the security credential, the store in communication with the authentication authority to validate the security credential (Par [0065]-[0066]; storing credential/ passwords);

an application program interface coupled to the client application, the application program interface operable to communicating regarding the validating of the token (Par [0061]-[0074],

[0104], [0114], [0130], [0150]; claims 1,12; client application/ interface using credentials/ token for mapping/ authentication) and

a server application operable on a second operating system to receive the token from the application program interface, the server application communicating with
the authentication authority to validate the token to enable the client application to
use services of the server application (Par [0104], [0114]-[0116], [0130]; Claims 1,12; 3rd party validating/ authenticating credentials).

Although Upton discloses use of a token as credentials (Par [0150]), and it would be further logically obvious to an ordinary skill in art to generate the token , Upton fails to disclose expressly the authentication authority further operable to generate a token.

However, Beck et al discloses the authentication authority further operable to generate a token (Par [0019]-[0024]; generating the user id token that would be used for authentication).

In the case position for inherency is not found supportable, the examiner notes that the reference Bhat et al discloses the authentication authority further operable to generate a token (Figure 6; Par 0030- 0079; especially Par 0035, 0066, 0077-0079; Claims 1-6; server system having token manager generating token). Bhat et al further discloses an authentication authority receiving the security credential from the security application program interface, the authentication authority further operable to communicate the token to the security application program interface where the security credential is valid, wherein the token contains user credentials encoded as a platform and application independent primitive data type (Par 0030-0079; claims 1-5; especially Par 0077-0079; token including string/ password, user identifying information; sending/ assigning token to application interface to authenticate user for particular application).

Bhat et al , Beck et al and Upton are analogous art because they are from the same field of authentication for network/ enterprise services. At the time of invention, it will be obvious to a person with ordinary skill in the art to combine the teaching of Bhat et al and/ or Beck et al with Upton to design the system wherein the authentication authority further operable to generate a token in order to facilitate an anonymous token based authentication.

Regarding claim 9, it is rejected applying as same motivation and rationale as applied above rejecting claim 1, furthermore, Upton discloses A method for providing application-to-application enterprise security, the method comprising:

communicating a security credential from a client application operable on a first operating system to an authentication authority (Par [0061]-[0074], [0127]-[0130], [0130], [0150]; Claims 1,12; client application/ interface providing credentials; service provider interface/ SPI authenticating public/ password type, or generic/ token type credentials);

communicating information related to the security credential between the authentication authority and a data store to determine whether the security credential is valid; wherein the token contains user credentials encoded as a platform and application independent primitive data type (Par [0104], [0114], [0130], [0150]; Claims 1,12; service provider interface/ SPI; validating/ authenticating credentials);

communicating the token to the client application; providing, by the client application, the token to a server application, the server application operable on a second operating system (Par [0061]-[0074], [0127]-[0130], [0130], [0150]; Claims 1,12; client application/ interface providing credentials; service provider interface/ SPI authenticating public/ password type, or generic/ token type credentials) ; and

validating, by the server application, the token before providing access to services of the server application by the client application (Par [0104], [0114]-[0116], [0130]; Claims 1,12; 3rd party validating/ authenticating credentials).

Upton fails to disclose expressly generating a token by the authentication authority when the security credential is valid.

However, Beck et al discloses generating a token by the authentication authority when the security credential is valid (Par [0024]; generating the token that would be used for authentication).

In the case position for inherency is not found supportable, the examiner notes that the reference Bhat et al discloses the authentication authority further operable to generate a token, wherein the token contains user credentials encoded as a platform and application independent primitive data type (Par 0031-0078; token)

Regarding claim 28, it recites the limitations of claims 1 and 9, therefore, it is rejected applying as above rejecting claim 1 and 9.

Regarding claim 2, Upton discloses the system of Claim 1, wherein the server application further comprises: an application program interface to communicate with the application program interface of the client application (Par [0061]-[0074], [0127]-[0130]; Claims 1 and 12; client application/ interface); and a security application program interface to communicate with the authentication authority (Par [0115],[0128]-[0130], [0145]-[0147]; security services; authentication/ authorization SPI).

Regarding claim 3, Beck et al discloses wherein the server application is operable to cache the token after validating the token with the authentication authority such that when the client application requests service of the server application, via the application program interfaces of the client application, the server application uses the cached token to validate the client application (Par [0018]-[0120]; using generated/ stored token for authentication).

Regarding claim 4, modified Beck et al -Upton system fails to disclose wherein the token generated by the authentication authority comprises a string including at least a portion of the security credential.

However, Bhat et al discloses wherein the token generated by the authentication authority comprises a string including at least a portion of the security credential (Par [0031]-[0077]).

Bhat et al and Upton are analogous art because they are from the same field of authentication for network/ enterprise services. At the time of invention, it will be obvious to a person with ordinary skill in the art to combine the teaching of Bhat et al with modified Beck et al -Upton to design the system wherein the token generated by the authentication authority comprises a string including at least a portion of the security credential in order to provide alternative token generation method.

Regarding claim 5 and 6, Bhat et al discloses wherein at least a portion of the token is in Extensible Markup Language format (Par [0030]; token as a part of URL; using XML). Furthermore, the examiner takes an official notice on that at the time of invention use of XML for defining credential or token was well known in art. Therefore, it would be obvious to a person of ordinary skill in art to define token in XML format so that it can be used in XML type URL access requests.

Regarding claim 7, Beck et al discloses wherein the token includes information related to an expiration date of the token (Par [0003]-[0005]; claims 11, 20). Furthermore, Bhat et al discloses wherein the token includes information related to an expiration date of the token (Par 0031-0077).

Regarding claims 10-12 and 29, they recite the limitations of claims 1-3, 9 and 28, therefore, they are rejected applying as above rejecting claims 1-3, 9 and 28.

Regarding claims 13-14, 16-17, 19 and 21-23, they recite the limitations of claims 4-7 and 9, therefore, they are rejected applying as above rejecting claims 4-7 and 9.

Regarding claim 18, Bhat et al discloses wherein the token includes a portion of the security credential in a string format (Par 0066-0078)

Regarding claim 20, Bhat et al discloses wherein the token is encrypted (Par 0066-0078; encrypted token).

Regarding claim 24, Upton discloses wherein the security credential is further defined as including a password and user identification (Par [0061]-[0074], [0150]). *Furthermore,* Bhat et al discloses wherein the security credential is further defined as password and user identification (Par 0035, 0066, 0077)

Regarding claim 25, it recites the limitations of claim20 and 24, therefore, it is rejected applying as above rejecting claims 20 and 24.

Regarding claims 30-33, they recite the limitations of claims 4-7 and 28, therefore, they are rejected applying as above rejecting claims 4-7 and 28.

Conclusion

10. References have not applied to reject, however found closely related to the claimed invention are:

Silhavy et al (US 2005/0108521 A1) discloses access control in a client (database) application based on client token generated previously by server/ security service.

Perlin et al (US 2006/01743334 A1) discloses access control to the application environment based on security tokens comprising application and user information.

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for response to this action is set to expire in 3 (Three) months and 0 (Zero) days from the mailing date of this letter. Failure to respond within the period for response will result in ABANDOMENT of the application (see 35 U.S.C 133, M.P.E.P 710.02(b)).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shanto M Z Abedin whose telephone number is 571-272-3551. The examiner can normally be reached on M-F from 9:00 AM to 5:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser, can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shanto M Z Abedin

Examiner, A.U. 2136

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136